UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/060,780 | 01/30/2002 | Travis Myron Cossel | 10012156-1 | 8265 |

7590 03/14/2006

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

| EXAMINER |
|---|
| SHAW, YIN CHEN |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2135 | |

DATE MAILED: 03/14/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

| **Advisory Action Before the Filing of an Appeal Brief** | **Application No.** 10/060,780 | **Applicant(s)** COSSEL ET AL. | |
|---|---|---|---|
| | **Examiner** Yin-Chen Shaw | **Art Unit** 2135 | |

***--The MAILING DATE of this communication appears on the cover sheet with the correspondence address --***

THE REPLY FILED 24 February 2006 FAILS TO PLACE THIS APPLICATION IN CONDITION FOR ALLOWANCE.

1. ☒ The reply was filed after a final rejection, but prior to or on the same day as filing a Notice of Appeal. To avoid abandonment of this application, applicant must timely file one of the following replies: (1) an amendment, affidavit, or other evidence, which places the application in condition for allowance; (2) a Notice of Appeal (with appeal fee) in compliance with 37 CFR 41.31; or (3) a Request for Continued Examination (RCE) in compliance with 37 CFR 1.114. The reply must be filed within one of the following time periods:
   a) ☐ The period for reply expires _____months from the mailing date of the final rejection.
   b) ☒ The period for reply expires on: (1) the mailing date of this Advisory Action, or (2) the date set forth in the final rejection, whichever is later. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of the final rejection.

   Examiner Note: If box 1 is checked, check either box (a) or (b). ONLY CHECK BOX (b) WHEN THE FIRST REPLY WAS FILED WITHIN TWO MONTHS OF THE FINAL REJECTION. See MPEP 706.07(f).

Extensions of time may be obtained under 37 CFR 1.136(a). The date on which the petition under 37 CFR 1.136(a) and the appropriate extension fee have been filed is the date for purposes of determining the period of extension and the corresponding amount of the fee. The appropriate extension fee under 37 CFR 1.17(a) is calculated from: (1) the expiration date of the shortened statutory period for reply originally set in the final Office action; or (2) as set forth in (b) above, if checked. Any reply received by the Office later than three months after the mailing date of the final rejection, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

NOTICE OF APPEAL

2. ☐ The Notice of Appeal was filed on _____. A brief in compliance with 37 CFR 41.37 must be filed within two months of the date of filing the Notice of Appeal (37 CFR 41.37(a)), or any extension thereof (37 CFR 41.37(e)), to avoid dismissal of the appeal. Since a Notice of Appeal has been filed, any reply must be filed within the time period set forth in 37 CFR 41.37(a).

AMENDMENTS

3. ☐ The proposed amendment(s) filed after a final rejection, but prior to the date of filing a brief, will not be entered because
   (a) ☐ They raise new issues that would require further consideration and/or search (see NOTE below);
   (b) ☐ They raise the issue of new matter (see NOTE below);
   (c) ☐ They are not deemed to place the application in better form for appeal by materially reducing or simplifying the issues for appeal; and/or
   (d) ☐ They present additional claims without canceling a corresponding number of finally rejected claims.

   NOTE: _____. (See 37 CFR 1.116 and 41.33(a)).
4. ☐ The amendments are not in compliance with 37 CFR 1.121. See attached Notice of Non-Compliant Amendment (PTOL-324).
5. ☐ Applicant's reply has overcome the following rejection(s): _____.
6. ☐ Newly proposed or amended claim(s) _____ would be allowable if submitted in a separate, timely filed amendment canceling the non-allowable claim(s).
7. ☒ For purposes of appeal, ~~the proposed amendment(s): a) ☐ will not be entered, or b) ☐ will be entered and an explanation of how the new or amended claims would be rejected is provided below or appended~~.

   The status of the claim(s) is (or will be) as follows:
   Claim(s) allowed: _____.
   Claim(s) objected to: _____.
   Claim(s) rejected: 1-23
   Claim(s) withdrawn from consideration: _____.

AFFIDAVIT OR OTHER EVIDENCE

8. ☐ The affidavit or other evidence filed after a final action, but before or on the date of filing a Notice of Appeal will not be entered because applicant failed to provide a showing of good and sufficient reasons why the affidavit or other evidence is necessary and was not earlier presented. See 37 CFR 1.116(e).
9. ☐ The affidavit or other evidence filed after the date of filing a Notice of Appeal, but prior to the date of filing a brief, will not be entered because the affidavit or other evidence failed to overcome all rejections under appeal and/or appellant fails to provide a showing a good and sufficient reasons why it is necessary and was not earlier presented. See 37 CFR 41.33(d)(1).
10. ☐ The affidavit or other evidence is entered. An explanation of the status of the claims after entry is below or attached.

REQUEST FOR RECONSIDERATION/OTHER

11. ☒ The request for reconsideration has been considered but does NOT place the application in condition for allowance because: See Attached Continuation Sheet.
12. ☐ Note the attached Information Disclosure Statement(s). (PTO/SB/08 or PTO-1449) Paper No(s). _____
13. ☐ Other: _____.

Continuation of 11 does NOT place the application in condition for allowance because: Applicant's argument filed on Feb. 24, 2006 have been fully considered, but found not persuasive.

Examiner disagrees with Applicant's argument that Pang fails to show or suggest each of the elements of claim 1, and claims 9 and 16, which are to the extent that these claims incorporate subject matter similar in scope with that of claim 1. In particular, Applicant argues that each of the authentication agents is requested to authenticate "the" unauthenticated parameter. For Claims 1, 9 and 16, the authentication parameter presented in the claim language is analogous to the protected string disclosed in Pang et al.. Pang et al. disclose the request broker service such that it would break the protected string and forward various components to the appropriate providers for processing, which involves authenticating the component of the original protected string [If however the URL is associated with a protect string (i.e., as in this example), then that step 708, dispatcher 214 sends an authentication request (e.g. BASIC(GROUP1)JIM/MANAGER AND IP(IP_LIST) 192.6.25.3), to authentication engine 602 via the object request broker 282. At step 710, authentication engine 602 parses the authentication request into separate provider requests (e.g. BASIC(GROUP1)JIM/MANAGER, IP(IP_LIST) 192.6.25.3). At step 712, authentication engine 602 sends the provider requests to authentication host 604 via the object request broker 282 for distribution to the appropriate providers (lines 34-44, Col. 22). Providers are modules of code that are used to perform specific types of authentication (lines 66-67, Col. 19)]. Therefore, the teaching by Pang et al. would still meet the scope of the claim language, "all of the authentication agents have been requested to authenticate "the" authentication parameter", with the entire protected string is being considered as "the" parameter

As for Claims 2, and 17, Applicant argues that Pang describes the operation of a web application server and the processing of browser requests, which are not the same as authentication requests as set forth in claim 2. In particular, Applicant argues that the motivation for claim 2 makes no sense. Examiner disagrees with Applicant's argument. Pang et al. disclose the waiting feature as the waiting list for the browser request [If the revised browser request remains on the waiting list for more than a predetermined amount of time, listener 210 may remove the request from the waiting list and send a message to the browser 202 to indicate that the request could not be processed (lines 60-64, Col. 16)]. Even though the disclosure of the waiting time feature is not explicitly directed toward the claimed limitation, the feature of the waiting time for the response is analogous to the waiting time for request processing. To further indicate such equivalence, Examiner provides that the motivation for having the waiting-time feature as to improve the efficiency since any ordinary person in the art at the time of the invention would realize that the waiting for response without imposing any restriction would takes resource and results in the decrease of the efficiency of the system. Therefore, putting a limitation on the time for waiting of the authentication response would improve the efficiency, which is parallel to freezing up the resource as pointed out by Pang et al. in lines 7-14, Col. 13. Applicant is reminded that the U.S.C. 103(a) states a patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains.

As for Claims 7, 14, and 22, Applicant argues that it is not the case that Pang shows or suggests that upon start the authentication manager is unaware of how many of the authentication agents exist in association with the authentication system and that the authentication manger discovers the authentication agents. Examiner disagrees with Applicant's argument. Pang et al. disclose the providers (i.e., authentication agent) are module of codes that are used to perform specific types of authentication and are implemented as dynamically linked libraries (DLL's), which are loaded dynamically at the runtime [Providers are modules of code that are used to perform specific types of authentication. According to one embodiment of the invention, providers are implemented as dynamically linked libraries (DLLs). As such, the providers are loaded into and execute within the same address space as the authentication hosts to which they belong. The providers are preferably loaded dynamically at runtime (lines 66-67, Col. 19 and lines 1-5, Col. 20)]. Pang et al. also disclose that each provider contains a table of function pointers and a proprieties list, where the function pointer table provides pointers for a particular provider functions that may be accessed by the authentication host, and the property list describes the type of authentication information that are required for accessing the particular provider [Each provider contains a table of function pointers and a properties list. The function pointer table provides pointers to particular provider functions that may be accessed by the authentication host 604. The property list describes the type of authentication information (such as the identity of the user initiating the request for a cartridge) that are required for accessing the particular provider (lines 6-12, Col. 20)]. Pang et al. further disclose only when the authentication host calls the list of function pointers that the particular provider would be used in authenticating the authentication request [An authentication host can call the entry point to obtain a list of function pointers that can be used in authenticating a particular provider request (lines 15-17, Col. 20)]. In another word, only when the host calls the list of the function of pointers, it would then be capable of knowing how (where) to access the particular provider functions (the authentication host is not able to link and access to an authentication provider prior to the call because the exact amount of authentication providers required and their functions are not known. Only when authentication host is executed, then the authentication host would link to the exact number of required authentication providers for authenticating the request). Therefore, Pang et al. disclose the invention that meets the claim limitation that the authentication manager is not aware of how many authentication agents exist at the start and needs to discover the authentication agents.

As for Claims 5, 12, and 20, Pang et al. disclose the authentication module (provider) returning the authentication result, either as valid or invalid [Providers are modules of code that are used to perform specific types of authentication (lines 66-67, Col. 19). At step 718, each provider sends a response to the authentication engine via the authentication host 605 and the object request broker 282 (lines 52-55, Col. 22). At step 720, authentication engine 602 applies any logical operations that were associated with the authentication request (lines 57-59, Col. 22)]. In addition, Pang et al. also disclose the authentication module returning the authentication result, either as valid or invalid, for connection [A separate authentication module 240 may be utilized for each authentication mechanism (lines 64-65, Col. 7 and Fig. 2). Authentication modules for denying or allowing access to a session (lines 10-11, Col. 10). If the expected result is received from the user (i.e., authentication module 240 has authenticated a user), authentication module informs authentication manager 204 of the authentication (lines 30-33, Col. 10)]. Stoltz et al. further disclose the option of accepting or declining the request, e.g. connection request, such as accepting all the requests at all the time, part of the time, or by never accepting the request at all, by the authentication modules [Authentication modules 240 each have the option of accepting or declining responsibility for a particular connection. Authentication modules 240 may base their decision on other available system resources or settings (e.g., from services 230-238, external

databases, etc.). In one or more embodiments, an authentication module 240 can be configured to accept all users all of the time, to only accept connections with smart cards, or to only accept users with pseudo tokens, for example (lines 57-64, Col. 8)]. In particular, Stoltz et al. disclose the authentication task may be depending on the type of parameter information presented [For example, one authentication module may be utilized to authenticate a user based on a smart card while another authentication module may be utilized to authenticate a user based on a key or password or biometrics information (lines 22-26, Col. 9)]. Thus, an authentication module will verify the parameter to be valid only if the parameter information is of the type it is expected and a match is found between the inputted parameter information and the stored one. Whenever the parameter is of a different type, the authentication module will verify it as invalid or simply decline the authentication process [Authentication module 204 presents the message to the first authentication module 240. The first authentication module 240 looks up the token in a database to determine if the token is register with the system. If not (i.e., the first authentication module does not want to accept responsibility for the token/message), the first authentication module passes the token/message onto a second authentication module (lines 50-57, Col. 9)]. In another word, for the parameter of a different type, the authentication module is expected to return an invalid response, which is actually the valid response (e.g., the authentication module is configured to authenticate the password information, but it receives the biometric information as a parameter. It would be returning an invalid response. However, this invalid response is actually a valid result because the authentication module is not supposed to verify the biometric parameter information). Therefore, the prior art by Pang et al. and Stoltz et al. still teach the limitation of the claim language in Claims 5, 12, and 20.

Based on the reasons above, Applicant is reminded that the claim language needs to be futher amended and, thus, Examiner maintatins the prior rejection dated on Jan. 12, 2006.

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100